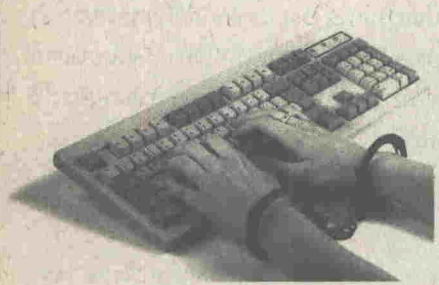
■ ปัญญา เปรมปรีดิ์

IT SECURITY
Computer - Network
Security and Information Protection



ประสบการณ์ในเรื่อง Computer Security

ศึกษาตัวปัญหาและศึกษาเทคนิคทางคอมพิวเตอร์ เมื่อเข้าใจแล้วเราจึงจะจัดการและปฏิบัติกันได้ถูกวิธี

เรื่องของความปลอดภัยในระบบคอมพิวเตอร์ (Computer Security) นี้ เป็นเรื่องที่ผมสนใจมาโดยตลอด เวลาไปดูงานที่ต่างประเทศผมจะต้องขอดูเรื่องนี้ด้วย และผมก็จะพบอยู่เสมอ ๆ ว่าเมืองไทยกับต่างประเทศนั้นคิดต่างกัน ความแตกต่างอันนี้แต่เดิมผมก็คิดว่ามาจากการมีประสบการณ์ที่แตกต่างกัน คือฝรั่งเขาถูกโกงกันบ่อย ๆ เขาจึงพัฒนาระบบการป้องกันและควบคุมที่รัดกุมมาก แต่คนไทยเรายังไม่เคยถูกโกง เราจึงปล่อยปะละเลยกันค่อนข้างมาก แต่มาในระยะหลัง ๆ นี้ คือหลังจากที่ผมได้ไปพูดให้กลุ่มคนหลาย ๆ กลุ่มฟัง เช่น กลุ่มผู้ตรวจสอบบัญชี (Auditor) กลุ่มนายธนาคาร กลุ่มนักคอมพิวเตอร์ แล้วผมก็รู้สึกว่า ปัญหามันน่าจะมาจากความไม่เข้าใจของพวกเรามากกว่า ระบบการป้องกันภัยในระบบคอมพิวเตอร์นี้ยุ่งยากและซับซ้อนเกินไปสำหรับคนทั่ว ๆ ไปที่จะเข้าใจได้ เรื่องนี้เป็นอย่างไรเรามาฟังกันดู

ผมอยากจะเริ่มต้นด้วยการเล่าให้ฟังเสียก่อนว่าฝรั่งเขาทำงานกันอย่างไร ศูนย์คอมพิวเตอร์ของฝรั่งนั้นส่วนใหญ่จะอยู่ลึกลงไปในชั้นใต้ดิน การควบคุมการเข้าออกนั้นเข้มงวดมาก คุณต้องนัดหมายเอาไว้ล่วงหน้า และเมื่อไปถึงแล้วจะต้องมีพนักงานต้อนรับมานำไป การเข้าออกต้องเซ็นชื่อและติดเบอร์ บางแห่งนั้นคนนำมาก็ไม่สามารถจะเข้าไปในศูนย์คอมพิวเตอร์ได้ อย่างเช่นที่ธนาคารขนาดใหญ่ ๆ ของเม็กซิโก เขาจะมีคนมารับช่วงในการนำชม เขาจัดสิ่งที่จะให้ชมเอาไว้เรียบร้อย มีการนำเข้าไปฟังบรรยายเสียก่อน แล้วจึงพาไปชมเครื่อง ชมระบบสื่อสาร ชมระบบไฟฟ้าสำรอง ... ฯลฯ เวลาที่ผมไปเจอกับศูนย์ที่อยู่ใต้ดิน ผมก็จะถามเขาว่าไม่กลัวเรื่องไฟไหม้และน้ำท่วมหรือ? ซึ่งเขาจะพาไปดูระบบไฟฟ้าสำรอง ระบบสูบน้ำ ระบบหมุนเวียนอากาศของเขา เวลาที่ผมไปเจอกับศูนย์ที่อยู่เหนือดินผมก็จะถามเขาว่าไม่กลัวเรื่องแผ่นดินไหวหรือ? ซึ่งเขาจะพาไปชมบนดาดฟ้าว่าศูนย์ของเขาอยู่ในที่โล่งแจ้ง และตัวอาคารมีการออกแบบให้แข็งแรงเป็นพิเศษ ศูนย์ประเภทนี้มักจะอยู่นอกเมือง และระบบสื่อสารนั้นอาศัยจานดาวเทียมเป็นสายหลัก แต่เขาก็มีเคเบิลเป็นสายสื่อสารสำรองด้วย (สมัยนี้ก็คงหันมาใช้ไฟเบอร์ออปติกกันหมดแล้ว)

มีอยู่สิ่งหนึ่งที่น่าสังเกตในเรื่องการเยี่ยมชมศูนย์คอมพิวเตอร์ของฝรั่ง คือถ้าเราบอกไปกว้าง ๆ ว่าจะชมศูนย์คอมพิวเตอร์ เขาก็จะพาไปชมแต่ตัวเครื่องและอุปกรณ์สนับสนุน และเมื่อเราถามถึงพวกโปรแกรมเมอร์เขาก็จะงุนงงไปหน่อยหนึ่ง ปัญหาก็คือ ฝรั่งนั้นบางทีเขาก็ไม่มีศูนย์ในด้านการพัฒนาระบบ เขาใช้วิธีจ้างทำ บางแห่งก็กระจายงานพัฒนาระบบไปอยู่ในฝ่ายงานต่าง ๆ บางฝ่ายก็พัฒนาโปรแกรมเอง บางฝ่ายก็จ้างทำ แต่บางแห่งก็มีศูนย์พัฒนาโปรแกรม ซึ่งมักจะแยกออกไปอยู่คนละแห่งกับตัวศูนย์เครื่องคอมพิวเตอร์ ที่เม็กซิโกนั้นส่วนใหญ่มีศูนย์พัฒนาโปรแกรมเป็นของตนเอง ธนาคารในสหรัฐฯ ครึ่งหนึ่งก็มีศูนย์พัฒนาโปรแกรมเป็นของตนเอง ธนาคารในอังกฤษมักจะอาศัยบริษัทผู้ผลิตฮาร์ดแวร์ คือผู้ผลิตฮาร์ดแวร์จะมีศูนย์

พัฒนาซอฟต์แวร์อยู่ด้วย ที่อังกฤษนั้นเมื่อเราขอไปดูศูนย์ด้านซอฟต์แวร์ก็ต้องนั่งรถออกไปเกือบ 100 ไมล์

ที่เม็กซิโกนั้นผมได้ไปเยี่ยมชมศูนย์พัฒนาโปรแกรมด้วย มันอยู่ประมาณชั้น 4 ถึงชั้น 6 3 ธนาคารคิดเหมือน ๆ กัน คือเขาจะจัดแบ่งเป็นกลุ่ม ๆ กลุ่มเหล่านี้จะถูกกั้นไว้ด้วยโต๊ะและแผงกั้น (partitions) แต่ละกลุ่มจะมีสีเฉพาะ ทางเดินที่ผ่านเข้าไปนั้นจะมีแถบสีอยู่ที่พื้น บัตรที่ติดหน้าอกของพนักงานและผู้เข้ามาเยี่ยมชมนั้นจะมีสี สีเหล่านี้แบ่งระดับการรักษาความปลอดภัย นั่นคือสีระดับสูงจะเข้าไปได้ทุกส่วน สีระดับต่ำจะเข้าไปแต่ส่วนที่อนุญาตให้เข้าไปเยี่ยมเยียนได้ พวกโปรแกรมเมอร์และนักวิเคราะห์ระบบเหล่านี้ก้มหน้าก้มตาทำงานกันอย่างคร่ำเคร่ง เขาจะมีห้องพักผ่อน ซึ่งมีเครื่องดื่มและขนมขาย เขามักจะไปพบปะและพูดคุยกันที่นั่น แต่เมื่อถามเขาว่าการประชุมและชี้แจงรายละเอียดของงานนั้นทำกันอย่างไร เขาก็บอกว่าโดยบันทึกและอีเมล์ แต่ส่วนใหญ่จะควบคุมโดยแบบฟอร์มที่มาจากซอฟต์แวร์ที่ช่วยพัฒนาระบบ ทุกอย่างจึงมีบันทึกเป็นหลักฐานที่จะให้ค้นดูการเปลี่ยนแปลงต่าง ๆ ได้ เรื่องด่วนบางอย่างก็ใช้วิธีติดที่กระดานประกาศ (Annoucement Board) ประเทศเม็กซิโกนี้ใช้คนในการพัฒนาซอฟต์แวร์มากพอ ๆ กับคนไทย ศูนย์ด้านพัฒนาโปรแกรมจึงใหญ่โตและแออัดเหมือน ๆ กัน แต่เขาจัดระบบการรักษาความปลอดภัยไว้ค่อนข้างดี มันจึงเป็นระเบียบมากกว่าเรา สำหรับเมืองมะริกันนั้นหาศูนย์ซอฟต์แวร์ขนาดใหญ่ (150 คนขึ้นไป) ได้ยากมาก บางแห่งใช้คฤหาสน์เก่า ๆ ขนาดใหญ่ ๆ (10 ห้อง) ที่อยู่นอกเมืองเป็นศูนย์พัฒนาซอฟต์แวร์ เวลาไปเยี่ยมชมจะต้องผ่านยามที่ประตูทางเข้า อาคารที่ทำงานนั้นมีทางเข้าทางเดียว มีพนักงานต้อนรับอยู่ที่นั่น แต่จะมีทางออกได้หลายทาง (ประตูครัว ประตูออกไปสวนดอกไม้ ฯลฯ) ทางออกเหล่านี้จะล็อกอัตโนมัติ มันเปิดได้จากภายในเท่านั้น ซึ่งผมเห็นว่าหละหลวมไปหน่อย ทั้งนี้เพราะคนภายในอาจเปิดรับคนภายนอกได้ แต่เมื่อถามถึงด้านการป้องกันภัยของซอฟต์แวร์ เขาก็บอกว่ามันอยู่ที่ระบบจัดการภายใน คือซอฟต์แวร์นั้นอยู่ในจานแม่เหล็ก คนที่พัฒนาโปรแกรมไหนก็จะเรียกออกมาได้แต่โปรแกรมนั้น เมื่อสั่งให้เซฟ ระบบก็จะก๊อบปี้ของเก่าขึ้นเทป และเก็บตัวใหม่ลงไว้ในจานแม่เหล็ก ในการเก็บลงไว้ในจานแม่เหล็กนี้จะทำการเข้ารหัส (encryption) ด้วยก็ได้ มันขึ้นอยู่กับความสำคัญของงานนั้น ๆ โปรแกรมเมอร์สามารถขอให้ไปเอาฉบับย้อนหลัง (บอกวันที่) กลับมาลงใหม่ได้ เครื่องเมนเฟรมที่ควบคุมเวอร์ชันของซอฟต์แวร์นี้มักจะอยู่คนละที่กับที่ทำงานของโปรแกรมเมอร์

นั่นเป็นการปฏิบัติงานของศูนย์คอมพิวเตอร์และศูนย์พัฒนาซอฟต์แวร์ ในด้านการใช้ระบบงาน หรือคือในบริเวณที่ทำงานของยูสเซอร์นั้นเขาก็มีการจัดการควบคุมเป็นอย่างดี เขามักจะแบ่งเป็น 2 พื้นที่ (zone) พื้นที่ที่ 1 นั้นคือที่ตั้งของตัวควบคุมการสื่อสารและเครื่องพิมพ์รายงานต่าง ๆ พื้นที่ส่วนนี้กั้นด้วยผนังกระจก คนเข้าออกต้องกดรหัสผ่านที่ประตู ส่วนพื้นที่ที่ 2 คือพื้นที่ทำงานของพนักงาน ซึ่งจะมีเทอร์มินัลและอุปกรณ์พ่วงต่าง ๆ เท่าที่จำเป็นในการทำงาน หรือให้บริการลูกค้า แต่ผมก็เห็นมีบางธนาคารที่เขาไม่มีพื้นที่ที่ 1 คือเขาย้ายเอาตัวควบคุมการสื่อสารและเครื่องพิมพ์ไปไว้ที่ศูนย์คอมพิวเตอร์ที่ส่วนกลาง แต่ละสาขาหรือแต่ละฝ่ายงานก็จะมีแต่เทอร์มินัลและตู้สายโทรศัพท์เท่านั้น เขาบอกว่าทำให้ดูแลได้ง่ายขึ้น แต่อย่างไรก็ตาม จุดสำคัญที่เขาใช้ควบคุมความปลอดภัยก็คือ การใช้บัตรควบคุม (control card หรือ ID card) ในการเข้าใช้เทอร์มินัล บัตรพวกนี้จะเก็บไว้ที่ผู้ควบคุมงาน ในตอนเช้าจะมีการบันทึกรหัสผ่าน (password) ลงไป พนักงานมาถึงที่ทำงานแล้วต้องไปเบิกบัตรควบคุมนี้ ได้มาแล้วต้องไปเปิดการทำงานของเทอร์มินัลซึ่งต้องรูดบัตรดังกล่าวนี้ที่เทอร์มินัล การเปลี่ยนรหัสผ่านใหม่ทุก ๆ วันจะช่วยป้องกันไม่ให้ใครเอาบัตรเก่าหรือบัตรปลอมมาใช้ บัตรควบคุมเหล่านี้จะแบ่งเป็น 2 หรือ 3 ระดับ ระดับแรกคือพนักงานที่ทำรายการปกติตามเทอร์มินัลต่าง ๆ เขาจะทำได้ตามเงื่อนไขปกติเท่านั้น เช่น บางคนที่ทำรายการเงินแห้งได้อย่างเดียว บางคนทำรายการได้ทั้งเงินแห้งและเงินสด แต่ทั้งหมดนี้จะทำได้ครั้งละไม่เกิน x ดอลล่าร์ ถ้าเกินนั้นก็จะต้องไปขอผู้ถือบัตรระดับที่ 2 มารูดบัตรเพื่ออนุญาต สำหรับบัตรระดับที่ 3 นั้นจะเป็นผู้ทำรายการพิเศษอื่น ๆ เช่น การสั่งโอนเงินชนิดมีผลทันที หรือโอนเงินไปเข้าบัญชีลูกค้าที่ธนาคารอื่น แต่

บางธนาคารเขาก็ใช้บัตรระดับที่ 2 แทน 3 ไปเลย ซึ่งจะทำให้เข้าใจได้ง่าย คือพนักงานจะแบ่งเป็น 2 ระดับเท่านั้น เขาเรียกว่าเทอร์มินัลโอเปอเรเตอร์ กับซูเปอร์ไวส์เซอร์ มันเป็นการควบคุมภายในของระบบ ทุก ๆ เย็นเมื่อพนักงานเหล่านี้บอกเลิกใช้เทอร์มินัล (sign-off หรือ log-off) แล้วก็ต้องนำบัตรควบคุมไปคืนที่ผู้ควบคุมงาน ผู้ควบคุมงานจะทำการปิดระบบงานและทำรายงานให้ผู้จัดการสาขาหรือผู้อำนวยการฝ่ายทราบ รายงานจะบอกสถานะของระบบงาน ในกรณีที่มีเหตุผิดปกติ เช่น ยอดเงินไม่ยัน ระบบงานบอกว่าไฟล์บางไฟล์ไม่ถูกต้อง ผู้ควบคุมงานกับผู้จัดการสาขาหรือผู้อำนวยการฝ่ายก็จะต้องดำเนินการแก้ไขตามคู่มือที่มีไว้ ถ้าแก้ไขไม่ได้ก็ต้องแจ้งให้ศูนย์คอมพิวเตอร์หรือทีมสนับสนุน (user support group) มาจัดการ ซึ่งจะเป็นเรื่องใหญ่มาก พวกนี้เข้ามาทำอะไรบ้างต้องจดบันทึกเอาไว้ ส่วนใหญ่แล้วจะต้องมีคนจากฝ่ายตรวจสอบกิจการภายใน (Audit Department) เข้ามาร่วมดูด้วย

ที่เล่ามานี้เป็นภาพจากภายนอก ซึ่งพวกเราที่ไปขอดูงานพอจะมองเห็นได้ แต่จริง ๆ แล้วก็จะมีสิ่งที่อยู่ลึกลงไปในระบบงานอีกมาก พวกนี้หาดูได้จากตำราและการได้ร่วมติดตั้งระบบงาน ผมได้มีโอกาสร่วมติดตั้งระบบงาน 3-4 เรื่องใหญ่ ๆ เช่น ระบบบริการออนไลน์ของธนาคารพาณิชย์ ระบบบัญชีรวม (general ledger) ระบบบัตรเครดิตวีซ่า ระบบการซื้อขายเงินตราต่างประเทศ ระบบการโอนเงินรายใหญ่ระหว่างธนาคารกับธนาคาร ในการทำงานเหล่านี้เราจะได้เห็นวิธีการป้องกันภัยของระบบที่ละเอียดยิ่งขึ้น ผมจะขอนำมาเล่าให้ฟังอย่างย่อ ๆ เสียหน่อยหนึ่ง

ในระบบบริการฝากถอนออนไลน์และผ่านเครื่องเอทีเอ็ม (ATM, Automatic Teller Machine) นั้น จุดที่ต้องระวังเพิ่มก็คือ สายสื่อสารที่เชื่อมโยงระหว่างเครื่องคอมพิวเตอร์กับตัวควบคุมที่สาขาต่าง ๆ สายสื่อสารเหล่านี้ผ่านไปตามชุมสายโทรศัพท์และตามชายคาบ้านเรือนต่าง ๆ มันจึงเปิดโอกาสให้ผู้ร้ายดักฟังและส่งข้อมูลเข้ามาสร้างเป็นรายการเท็จได้ ดังนั้นเขาจึงต้องมีการเข้ารหัส (encryption) ก่อนส่งออก และถอดรหัส (decryption) เมื่อรับสัญญาณเข้ามา สูตรในการเข้ารหัสและถอดรหัสเหล่านี้เขามักจะใช้ชนิดที่ใช้กุญแจรหัส (encryption key) ตัวเดียวกัน เราเรียกสูตรแบบนี้ว่า "สูตรสมมาตร" (symmetric encryption algorithm) สูตรแบบนี้มันเหมือนกันทั้งด้านเข้ารหัสและถอดรหัส มันเป็นคุณสมบัติพิเศษอันหนึ่งที่ทำให้ไม่ต้องเขียนโปรแกรมแยกเป็น 2 ด้าน สูตรแบบนี้ที่เรารู้จักกันดีคือดีอีเอส (DES = Data Encryption System) ซึ่งเผยแพร่โดยสหรัฐอเมริกา และธนาคารพาณิชย์ต่าง ๆ มักจะใช้กัน แต่สูตรนี้ก็มีข้อเสีย คือมันใช้เวลาในการคำนวณค่อนข้างสูง มันลดเวลาในการคำนวณได้ด้วยการลดความยาวของกุญแจรหัส แต่เมื่อลดลงแล้วก็จะทำให้คนใช้เครื่องเพื่อค้นหากุญแจรหัส (break the encryption) ได้ง่าย บริษัทผู้ผลิตโปรแกรมบริการฝากถอนออนไลน์จึงทิ้งให้ผู้ซื้อเป็นคนตัดสินใจเอง คือจะใส่การเข้ารหัสถอดรหัส หรือไม่ใส่ก็ได้ และผู้ซื้อต้องติดต่อและขออนุญาตจากรัฐบาลสหรัฐฯ เอง

ในระบบบัญชีรวม (general ledger) ของธนาคารนั้นก็เหมือน ๆ กันกับระบบฝากถอน คือข้อมูลจากสาขาต่าง ๆ อาจส่งผ่านทางออนไลน์มาก็ได้ ถ้าผ่านทางออนไลน์ก็จะต้องคิดว่าควรทำการเข้ารหัสและถอดรหัสหรือไม่ แต่ที่ผมได้สัมผัสมานั้นธนาคารเขาส่งข้อมูลเข้ามาเป็นแผ่น ๆ วันละ 1 ชุด ประมาณ 3 หน้ากระดาษ แล้วต้องมาคีย์ข้อมูลเข้าระบบที่สำนักงานใหญ่ มันจึงไม่จำเป็นต้องเข้ารหัส

ระบบบัตรเครดิตนั้นมีจุดที่ต้องระมัดระวังมากที่สุดอยู่ที่การทำบัตร บัตรเครดิตจะมีแถบแม่เหล็กเอาไว้บันทึกชื่อ หมายเลขบัตร และข้อมูลที่จะเอาไว้เช็กว่าเป็นบัตรออกโดยบริษัทหรือธนาคารที่เป็นตัวแทนบริษัท เจ้าข้อมูลเพื่อเอาไว้ตรวจเช็กนั้นจะต้องคำนวณโดยสูตรเข้ารหัสเช่นกัน และบริษัทบัตรเครดิตส่วนใหญ่ก็จะใช้สูตรเข้ารหัสแบบสมมาตร แต่เขาจะใช้กุญแจเข้ารหัสที่มีความยาวสูง ทั้งนี้เพราะบัตรที่ออกให้กับลูกค้าไปแล้วนั้นไม่สามารถจะเรียกกลับมาเข้ารหัสใหม่ได้ กุญแจเข้ารหัสนี้เขามักจะตัดแบ่งออกเป็น 4 ส่วน แต่ละส่วนบันทึกลงไว้ในแผ่นดิสก์เกตต์ ซึ่งเมื่อส่งมอบมาให้ธนาคารแล้วจะต้องแยกเก็บอยู่ในความดูแลของผู้บริหารระดับสูง นี่จะทำให้ผู้บริหารเหล่านี้ไม่สามารถขโมยไปใช้ทำบัตรปลอมได้ ท่านผู้อ่านควรสังเกตว่าบัตรเครดิตนี้ราคาแผ่นละไม่ถึง 60 บาท และเครื่องมือที่จะบันทึกข้อมูลลงในแถบแม่เหล็ก (encoder) ก็ราคาไม่ถึงหมื่นบาท การทำบัตรปลอมจึงเป็นเรื่องง่าย ถ้าสามารถรู้กุญแจที่ใช้เข้ารหัส การปลอมโดยทำสำเนาจากบัตรจริงนั้นเขาไม่กลัว ทั้งนี้เพราะเจ้าของบัตรจะต้องรีบแจ้งว่าบัตรหาย และเขาสามารถระงับการใช้บัตรเหล่านี้ภายใน 1-2 วัน ความเสียหายนั้นผู้ทำบัตรหายจะต้องรับผิดชอบอยู่แล้ว มองที่จุดนี้แล้วจะเห็นได้ว่าบริษัทผู้ออกบัตรนั้นเขากลัวตัวแทนจะโกงเขามากกว่าผู้ร้ายทั่วไป แต่อย่างไรก็ตาม ตัวกุญแจเข้ารหัสนี้เขาก็พยายามเปลี่ยนอยู่เสมอ ๆ และบัตรก็มีอายุแค่ 1 หรือ 2 ปี ดังนั้นมันจึงเป็นระบบที่มีการป้องกันที่ดีพอสมควร

ระบบการซื้อขายเงินตราต่างประเทศนั้นถ้าเรามองดูจำนวนเงินที่ซื้อขายหรือโอนให้แก่กันและกันนั้น จะเป็นก้อนโตมาก ดังนั้นบางคนจึงอาจคิดว่ามีระบบป้องกันภัยที่ดีเยี่ยม แต่ในความเป็นจริงแล้ว การซื้อขาย กับการโอนเงินเพื่อชำระหนี้กันจริง ๆ นั้นถูกแยกออกจากกัน การซื้อขายเป็นแค่การทำสัญญาด้วยวาจาเท่านั้น ซึ่งเขาจะใช้การบันทึกเสียงลงบนเทปเป็นเครื่องมือในการป้องกันและโต้แย้ง แต่อย่างไรก็ตาม การที่จะเข้าถึงข้อมูลการเสนอซื้อเสนอขายนั้นมันต้องผ่านเครือข่ายการสื่อสารที่ชมรมตั้งขึ้นมา มันจึงมีการควบคุมและป้องกันอยู่ที่ระบบนั้นด้วย กล่าวคือ การเชื่อมโยงเข้าสู่เครือข่ายนั้นต้องมีรหัสผ่าน (password) คนที่ได้รับมอบหมายจากธนาคารและสถาบันการเงินที่เป็นสมาชิกเท่านั้นที่จะมีรหัสผ่านเหล่านี้ การส่งข้อมูลไปมา (โดยเฉพาะอย่างยิ่งในขั้นตอนการ log-in) นั้นจะต้องเข้ารหัส และพวกนี้ก็ใช้สูตรชนิดสมมาตรเช่นกัน สำหรับด้านการสั่งโอนเงินตามที่ได้ตกลงซื้อขายกันนั้นเขามักจะทำผ่านเครือข่ายสวิฟต์ (SWIFT) ซึ่งเป็นเครือข่ายที่ตั้งขึ้นโดยกลุ่มธนาคารใหญ่ของยุโรปและสหรัฐฯ ธนาคารและสถาบันการเงินต่าง ๆ ต้องเข้าเป็นสมาชิก สมาชิกก็มีหลายระดับ คือสมาชิกระดับผู้ก่อตั้ง สมาชิกระดับมีอำนาจเต็ม และสมาชิกสมทบ สมาชิกเหล่านี้ต้องมีระบบเครื่องคอมพิวเตอร์และซอฟต์แวร์ตามที่เขากำหนดไว้ และสมาชิกเหล่านี้ต้องมีรหัสผ่าน (password) รหัสผ่านต่าง ๆ เหล่านี้จะถูกสร้างโดยศูนย์ควบคุมและส่งมอบไปให้สมาชิกต่าง ๆ ใช้ รหัสจะถูกเปลี่ยนอยู่เป็นประจำ ทั้งนี้เพื่อป้องกันมิให้ใครแอบค้นหากุญแจสร้างคำสั่งลวง แต่อย่างไรก็ตาม คำสั่งที่ผ่านมาจากสวิฟต์นั้นก็มิได้เข้าไปทำการหักบัญชีหรือเพิ่มยอดเงินโดยตรง มันต้องมีพนักงานที่จะดำเนินการหักบัญชีและโยกย้ายเงินจริง ๆ อีกต่อหนึ่ง ดังนั้นระบบการซื้อขายเงินตราต่างประเทศจึงมิได้มีการป้องกันอะไรที่เหนือไปกว่าระบบอื่น ๆ

จากที่เล่ามานี้เราจะเห็นได้ว่า การรักษาความปลอดภัยในระบบงานคอมพิวเตอร์นั้นเห็นได้ชัดเจนอยู่ 2 ลักษณะ ลักษณะแรกคือการป้องกันอาคารสถานที่และอุปกรณ์ต่าง ๆ อันนี้บางคนเรียกว่าการรักษาความปลอดภัยทางวัตถุ (physical security) ส่วนลักษณะที่ 2 คือการป้องกันการใช้โปรแกรมหรือเทอร์มินัลเพื่อแก้ไขเปลี่ยนแปลงข้อมูลภายในเครื่อง ส่วนนี้เขามักจะเรียกว่า การรักษาความปลอดภัยทางตรรก (logical security) ซึ่งคนไทยเราก็พอจะมองเห็นได้ เราจึงได้ลอกแบบมาจากฝรั่ง แต่หลาย ๆ แห่งก็ได้พยายามคิดและปรับเปลี่ยนไปตามสถานการณ์ เช่น เมืองไทยเรานั้นมีเหตุร้ายประเภทแผ่นดินไหวและน้ำท่วมน้อยมาก แต่ละครั้งก็ไม่มีความรุนแรงอะไรมาก ดังนั้นเราจึงมักจะติดตั้งเครื่องคอมพิวเตอร์และระบบสื่อสารเอาไว้บนชั้นที่อยู่เหนือดิน และเนื่องจากเรายังไม่มีปัญหาด้านการก่อการร้ายในเมือง เราก็เลยทำห้องคอมพิวเตอร์ให้โปร่งใส ทำเป็นห้องกระจกอย่างดี แล้วก็เปิดให้คนเข้าชมได้ ซึ่งจะได้ผลประโยชน์ทางด้านโฆษณา สำหรับการรักษาความปลอดภัยทางตรรกนั้นส่วนใหญ่ก็ลอกแบบจากฝรั่ง แต่เมื่อนำมาปฏิบัติแล้วก็จะพบว่า มีความหละหลวมเกิดขึ้นโดยทั่วไป เช่น บัตรควบคุมในระดับซูเปอร์ไวส์เซอร์นั้นปล่อยให้อยู่ในมือของเทอร์มินัลโอเปอเรเตอร์ รหัสผ่านสำหรับเข้าใช้เครื่องและสำหรับการเรียกใช้โปรแกรมจะถูกบอกต่อ ๆ กันไปในหมู่ผู้ปฏิบัติงานทุกคน และไม่มีการเปลี่ยนแปลงตามห้วงเวลาที่กำหนด เวลาโปรแกรมเมอร์หรือโอเปอเรเตอร์ลาออกก็ไม่มีการเรียกเก็บบัตรคืนมา และไม่มีการเปลี่ยนรหัสที่เครื่องควบคุมประตู เมื่อระบบงานเกิดขัดข้องจนถึงขั้นต้องแก้ไขโปรแกรมเราก็ให้โปรแกรมเมอร์แก้ไขโปรแกรมบนเครื่องที่ใช้งานจริงไปเลย และโปรแกรมล่าสุดนี้มักจะถูกเก็บไว้ในดิสก์เกตต์ของโปรแกรมเมอร์ ตัวสำเนาของศูนย์คอมพิวเตอร์ที่เก็บอยู่ในเทปแม่เหล็กนั้นก็จะไม่ใช่ตัวล่าสุด

ถึงแม้ว่าจะมีการปฏิบัติงานอย่างหละหลวม แต่ในเมืองไทยเรานั้นมีการทุจริตผ่านระบบงานคอมพิวเตอร์น้อยมาก ในช่วงเวลา 30 ปีที่ผมทำงานมา ผมได้ข่าวเพียง 3 เรื่องเล็ก ๆ ซึ่งมีดังนี้ เรื่องแรกคือ พนักงานเทลเลอร์ (บริการฝากถอนที่เทอร์มินัล) ได้อาศัยบัตรของซูเปอร์ไวส์เซอร์ทำรายการฝากเงินสดเกิน 500,000 บาท แล้วเดินทางไปถอนเงินที่สาขาอื่นในช่วงพักรับประทานอาหารเที่ยง แล้วไม่กลับมาทำงาน ซึ่งธนาคารไปตรวจพบในตอนเย็น จึงไม่สามารถจะสกัดกั้นได้ เรื่องนี้ธนาคารต้องแก้ไขด้วยการออกแนวปฏิบัติว่า การรับฝากเงินสดต่างสาขานั้นจะยังไม่ยอมให้ถอนเป็นเงินสดในวันเดียวกัน

แต่ก็เป็นการล้อมคอกหลังจากที่วัวได้หายไปแล้ว 1 ตัว เรื่องที่ 2 ที่ผมได้รับฟังมาคือ มีคนอาศัยการแอบมองดูหมายเลขรหัสของการถอนเงินจากเอทีเอ็มของผู้อื่น และเก็บใบสลิปที่ผู้ถอนทิ้งลงถังขยะไปทำบัตรปลอม ได้แล้วนำมาถอนเงินจากเครื่องเอทีเอ็ม เมื่อได้เงินไปใช้แล้วก็มาคุยโอ้อวดกับเพื่อน ๆ จนธนาคารทราบเรื่อง ธนาคารจึงแก้ไขโดยเลิกพิมพ์ข้อมูลบางอย่างบนสลิปของการถอนเงินจากเครื่องเอทีเอ็ม นี่ก็เป็นการล้อมคอกหลังจากวัวหายไปแล้วเช่นกัน เรื่องสุดท้ายคือ มีเด็กหนุ่มหัวใสเอาก้านไม้ขีดไฟชุบกาวลาเท็กซ์ไปเสียบกั้นช่องจ่ายเงินของเครื่องเอทีเอ็มเอาไว้ เมื่อมีคนมาถอนเงินก็จะไม่ได้เงินไป แต่เมื่อออกไปแล้วเด็กคนนั้นก็เอาลวดเหล็กมาเขี่ยเงินที่ค้างอยู่ในช่องจ่ายเงินออกไป การกระทำผิดนี้ทำซ้ำอยู่หลายหน จนกระทั่งพนักงานที่สาขามองเห็นได้จึงเข้าจับกุมและส่งให้ตำรวจดำเนินการต่อไป

จริง ๆ แล้วการทุจริตผ่านระบบงานคอมพิวเตอร์ในเมืองไทยนั้นก็คงจะมีมากกว่านี้ แต่เมื่อเทียบกับเรื่องเล่าในวารสารประเภทที่เกี่ยวกับการรักษาความปลอดภัยของสหรัฐฯ และยุโรปแล้วเรามีเหตุร้ายน้อยครั้งกว่า และในวงเงินที่เล็กกว่ามาก ดังนั้นจึงไม่ค่อยจะมีใครสนใจที่จะปรับปรุงหรือแก้ไข กลุ่มผู้ตรวจสอบ กลุ่มนักการธนาคาร และกลุ่มนักคอมพิวเตอร์ที่ผมได้สัมผัสมานั้นไม่แสดงความคิดเห็นใด ๆ เขาได้แต่พูดกันว่า การที่จะชี้แจงให้ซูเปอร์ไวส์เซอร์เข้าใจถึงความสำคัญของบัตรควบคุมและรหัสผ่านต่าง ๆ นั้นมันยาก พวกนี้ต้องการความคล่องตัว ซึ่งในตอนแรก ๆ ผมก็เห็นคล้อยตามไปด้วย แต่หลังจากที่ได้ทำงานในระบบงานที่สำคัญยิ่ง ๆ ขึ้น เช่น ระบบการโอนเงินระหว่างธนาคารต่าง ๆ ผมก็เริ่มจะรู้สึกว่าปัญหานั้นไม่ได้มาจากความต้องการความคล่องตัวแต่อย่างเดียว ปัญหามันมาจากความไม่เข้าใจในวิธีการทางด้านคอมพิวเตอร์ และไม่รู้เป้าหมายที่แท้จริงของการวางระบบความปลอดภัย เหตุผลของผมเป็นดังนี้

เอาเรื่องเป้าหมายของการรักษาความปลอดภัยเสียก่อน จริง ๆ แล้วการทุจริตต่าง ๆ นั้นส่วนใหญ่เกิดจากฝีมือคนภายใน ดังนั้นจึงต้องมุ่งเน้นที่การแบ่งแยกหน้าที่ การควบคุมตามลำดับความเชื่อถือได้ของคน และการสอบยันซึ่งกันและกันของคนในระดับเท่าเทียมกัน ยกตัวอย่างเช่น รหัสลับที่จะใช้ในการทำบัตรเครดิต สิ่งนี้สำคัญมาก ถ้าตกไปถึงมือคนภายนอกก็อาจทำให้บริษัทที่ออกบัตรเครดิตนั้นล่มจมได้ สิ่งที่สำคัญในระดับนี้ต้องแบ่งเป็นหลาย ๆ ส่วน แล้วให้ผู้บริหารระดับสูงเก็บเอาไว้คนละส่วน แต่คนไทยนั้นไม่ค่อยจะเข้าใจ บางทีก็ให้เลขาหน้าห้องถือไปส่งเข้าห้องคอมพิวเตอร์ และทุกครั้งก็อยู่ในมือของโอเปอเรเตอร์พร้อม ๆ กันทั้ง 4 แผ่น ตัวนายแบงค์เองก็ไม่ทราบว่าเรื่องนี้สำคัญถึงระดับคอขาดบาดตายจริง ๆ แล้วผู้บริหารควรมาเอง ต้องส่งเข้าไปทีละแผ่นและต้องระวังมิให้มีการสั่งก๊อบปี้ลงไว้ในเครื่อง

ในเรื่องของเป้าหมายการรักษาความปลอดภัยนี้จริง ๆ แล้วนอกจากจะป้องกันการเข้าถึงเครื่อง ป้องกันการใช้ระบบผิดวัตถุประสงค์ (physical security และ logical security) แล้ว มันยังมีเรื่องของการรักษาความโปร่งใส (fairness) อยู่ด้วย เรื่องนี้เป็นสิ่งที่คนไทยไม่เคยรู้จัก ไม่เคยคิด ไม่เคยคำนึงถึงมาก่อนเลย ผมจะขอเล่าถึงประสบการณ์ที่น่าช้ำใจของผมให้ฟัง คือตอนที่ผมย้ายไปทำงานที่ธนาคารแห่งประเทศไทยใหม่ ๆ นั้น ธนาคารพาณิชย์กำลังรวมเครื่องเอทีเอ็มให้เป็นเครือข่าย 2 เครือข่าย การรวมกันเป็นเครือข่ายนี้ก็ต้องมีการเชื่อมโยงเครื่องคอมพิวเตอร์ของธนาคารกับธนาคารเข้าหากัน ผมก็เลยเขียนเป็นบทความแหย่ดูว่าธนาคารเข้าใจปัญหาเรื่องการเชื่อมโยงเหล่านี้หรือไม่ คำถามของผมก็คือ ข้อมูลที่ผ่านสายสื่อสารที่เชื่อมระหว่างเครื่องคอมพิวเตอร์และเครื่องเอทีเอ็มเหล่านี้มีการเข้ารหัสหรือไม่ และเข้ารหัสแบบใด ผมพูดชี้นำไปว่าถ้าไม่มีการเข้ารหัสจะถูกโกงได้ ผมได้ยกตัวอย่างรูปภาพประกอบด้วย เมื่อเขียนไปลงวารสารแล้วก็ถูกผู้ว่าการธนาคารแห่ง

ประเทศไทยเรียกเข้าไปเทศนา ท่านบอกว่ามีนายธนาคารมาฟ้อง นายธนาคารเขาเห็นว่าเป็นการ "ชี้โพรงให้กระรอก" ซึ่งผมฟังดูแล้วรู้สึกเศร้าใจ คือแนวคิดของนายธนาคารนั้นมีอยู่ว่า ระบบป้องกันภัยนี้ควรเก็บเป็นความลับ และควรรู้กันแต่เฉพาะในหมู่สมาชิกเท่านั้น ซึ่งมันขัดกับหลักการทางด้านการรักษาความปลอดภัยโดยสิ้นเชิง เราไม่ได้อยู่ในยุคโบราณแล้ว ในสมัยกรุงศรีอยุธยานั้นมีการสร้างวัดพระพุทธบาทขึ้นมา และเพื่อเก็บเป็นความลับก็เลยต้องฆ่าช่างทุกคน ในยุคของอเล็กซานเดอร์มหาราชนั้นก็เช่นกัน สร้างระบบเข้ารหัสแบบเลื่อนตำแหน่งตัวอักษรขึ้นมา แล้วให้รู้กันแต่ในหมู่นักรบโรมันใครมารู้ความลับให้ฆ่าทิ้งเสีย แนวคิดแบบนี้มันล้าสมัยแล้ว ในปัจจุบันนี้สูตรการเข้ารหัสนั้นเขาให้เปิดเผยได้ (ถ้าจะปิดเป็นความลับก็ต้องฆ่าโปรแกรมเมอร์หลังจากเขียนโปรแกรมเสร็จ) แต่สิ่งที่จะทำให้คนร้ายปลอมคำสั่งไม่ได้นั้นอยู่ที่ตัวเลขที่เป็นกุญแจ ดังนั้นธนาคารควรประกาศไปเลยว่ามีการเข้ารหัส สูตรในการเข้ารหัสนั้นเป็นชนิดใด และมีความปลอดภัยมากน้อยแค่ไหน ผู้ใช้จะได้มีความรู้สึกมั่นใจในระบบเอทีเอ็มเหล่านั้น นอกจากนี้ จริง ๆ แล้วการเชื่อมโยงระหว่างธนาคารกับธนาคารนั้นต้องเข้ารหัสแบบไม่สมมาตร ทั้งนี้เพราะระบบแบบสมมาตรอย่าง "ดีอีเอส" (DES) นั้นผู้ส่งคำสั่งกับผู้รับคำสั่งนั้นใช้สูตรและกุญแจตัวเดียวกัน ดังนั้นผู้รับคำสั่งนั้นอาจสร้างคำสั่งปลอมขึ้นมาก็ได้ เมื่อใดที่เกิดการโต้แย้ง คือผู้ส่งบอกว่าไม่ได้ส่ง ผู้รับจะไม่สามารถพิสูจน์ความบริสุทธิ์ของฝ่ายตนได้ นี่เราเรียกว่าปัญหาด้านความโปร่งใส สูตรแบบไม่สมมาตร (อย่าง RSA เป็นต้น) เท่านั้นที่จะสามารถยืนยันได้ว่าเป็นคำสั่งมาจากธนาคารต้นทาง

แต่... เรื่องเหล่านี้ผมไม่สามารถจะนำมาอธิบายแก่สาธารณชนได้ ทั้งนี้เพราะท่านผู้ว่าการพูดอยู่อย่างเดียวว่า "อย่าเขียนบทความให้เป็นที่กระทบกระเทือนธนาคารพาณิชย์อีก" ผมก็เลยต้องเก็บอัดเอาไว้ในใจสิบกว่าปี

เรื่องของการไม่เข้าใจหลักการทางคอมพิวเตอร์ และไม่เข้าใจเป้าหมายของระบบป้องกันภัยนี้ผมยังมีอีกหลายเรื่อง เรื่องล่าสุดคือระบบการโอนเงินรายใหญ่ระหว่างธนาคารพาณิชย์และสถาบันการเงินต่าง ๆ ในระบบดังกล่าวนี้ผู้รับจ้างทำซอฟต์แวร์เขาเสนอให้ใช้การเข้ารหัสแบบสมมาตรเช่นกัน ซึ่งผมได้บอกให้ยูสเซอร์คิดให้ดี ๆ แต่ก็ไม่มีใครคิด และหลังจากที่เริ่มใช้ระบบไป 2-3 สัปดาห์ผมก็ถามอีกว่า ธนาคารพาณิชย์และธนาคารกลางเก็บหลักฐานอะไรไว้บ้าง ข้อมูลที่เก็บไว้นี้เป็นชนิดที่ยังไม่ได้ถอดรหัส (original input) หรือถอดรหัสแล้ว และกุญแจที่สร้างและใช้กันแต่ละวันนั้นเก็บไว้หรือไม่ ผมก็ได้รับคำตอบว่า เก็บแต่ที่ถอดรหัสแล้ว และไม่มีการเก็บกุญแจที่ใช้เอาไว้เลย พวกเขาอ้างว่าการโอนเงินเหล่านี้จะมีการตรวจสอบและยันกันทุก ๆ วัน เมื่อทุกธนาคารยืนยันแล้วก็ไม่ต้องมีหลักฐานอื่นใดเอาไว้ใช้ตรวจสอบ ซึ่งผมเห็นว่ามันไม่ถูกต้อง ทั้งนี้เพราะผู้ตรวจบัญชีภายนอกของธนาคารเหล่านี้อาจต้องมาขอดูหลักฐานเหล่านี้ได้ ถ้าไม่เก็บไว้ให้ครบถ้วนมันก็ไม่มีความโปร่งใสเพียงพอ ถ้าธนาคารใดธนาคารหนึ่งมากล่าวอ้างในภายหลังว่าเขาไม่ได้สั่งโอนเงินให้คนอื่นไป แล้วธนาคารกลางจะเอาอะไรมาพิสูจน์ความบริสุทธิ์ของตน

ปัญหาเรื่องความปลอดภัยในระบบคอมพิวเตอร์ (Computer Security) นี้คงจะต้องรอให้เกิดปัญหาจริง ๆ จัง ๆ กันเสียก่อน คนไทยเราคงต้องใช้เวลาในการศึกษาตัวปัญหาและศึกษาเทคนิคทางคอมพิวเตอร์อีกมาก เมื่อเข้าใจแล้วเราจึงจะจัดสร้างและปฏิบัติกันได้ถูกวิธี เรื่องแบบนี้เราคงต้องเสียเงิน (หรือที่บางคนเรียกว่าเสียค่าโง่) ไปเป็นหมื่น ๆ ล้านเสียก่อน แล้วจึงจะรู้สึก